

Certsuperior Certification Practice Statement

Version 4.1.0

Effective Date: 15/Nov/2016



Certsuperior S. de R.L. de C.V.
Av. Santa Fe # 170 Of. 3-2-06, Col. Lomas de Santa Fe.
Del. Alvaro Obregon, Mexico, D.F., C.P. 01210.

+52(55)59855000
www.certsuperior.com

Certsuperior Certification Practices Statement

© 2016 Symantec Corporation. All rights reserved.
Printed in the United States of America.

Published date: 15/Nov/2016

Important – Acquisition Notice

On August 9, 2010, Symantec Corporation completed the acquisition of VeriSign Inc's Authentication division. As a result Symantec is now the registered owner of this Certificate Practices Statement document and the PKI Services described within this document.

However a hybrid of references to both "VeriSign" and "Symantec" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark Notices

Symantec, the Symantec logo, and the Checkmark Logo are the registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. The VeriSign logo, VeriSign Trust and other related marks are the trademarks or registered marks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed by Symantec Corporation. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of Symantec Corporation.

Notwithstanding the above, permission is granted to reproduce and distribute this Certsuperior Certification Practices Statement on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to Symantec Corporation.

Requests for any other permission to reproduce this Certsuperior Certification Practices Statement (as well as requests for copies from Symantec) must be addressed to Certsuperior, Av. Santa Fe # 170 Of. 3-2-06, Col. Lomas de Santa Fe. Del. Alvaro Obregon, Mexico, D.F., C.P. 01210 Attn: Practices Development. Tel: +52(55)59855000 Fax: +52(55)50814376 Net: practices@certsuperior.com

Table of Contents:

1.	INTRODUCTION	1	4.4.3	Notification of Certificate Issuance by the CA to Other Entities.....	19
1.1	Overview	Error! Bookmark not defined.	4.5	Key Pair and Certificate Usage	19
1.2	Document name and Identification	3	4.5.1	Subscriber Private Key and Certificate Usage	19
1.3	PKI Participants.....	4	4.5.2	Relying Party Public Key and Certificate Usage.....	19
1.3.1	Certification Authorities.....	4	4.6	Certificate Renewal.....	20
1.3.2	Registration Authorities.....	5	4.6.1	Circumstances for Certificate Renewal	20
1.3.3	Subscribers.....	5	4.6.2	Who May Request Renewal	20
1.3.4	Relying Parties.....	5	4.6.3	Processing Certificate Renewal Requests	20
1.3.5	Other Participants.....	6	4.6.4	Notification of New Certificate Issuance to Subscriber	21
1.4	Certificate Usage.....	6	4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	21
1.4.1	Appropriate Certificate Usages	6	4.6.6	Publication of the Renewal Certificate by the CA	21
1.4.2	Prohibited Certificate Uses	7	4.6.7	Notification of Certificate Issuance by the CA to Other Entities.....	21
1.5	Policy Administration	7	4.7	Certificate Re-Key.....	21
1.5.1	Organization Administering the Document	7	4.7.1	Circumstances for Certificate Re-Key	21
1.5.2	Contact Person	8	4.7.2	Who May Request Certification of a New Public Key	21
1.5.3	Person Determining CP Suitability for the Policy.....	8	4.7.3	Processing Certificate Re-Keying Requests.....	22
1.5.4	CPS Approval Procedure.....	8	4.7.4	Notification of New Certificate Issuance to Subscriber	22
1.6	Definitions and Acronyms.....	8	4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate	22
2.	Publication and Repository Responsibilities	8	4.7.6	Publication of the Re-Keyed Certificate by the CA	22
2.1	Repositories	8	4.7.7	Notification of Certificate Issuance by the CA to Other Entities.....	22
2.2	Publication of Certificate Information.....	9	4.8	Certificate Modification	22
2.3	Time or Frequency of Publication.....	10	4.8.1	Circumstances for Certificate Modification	22
2.4	Access Controls on Repositories	10	4.8.2	Who May Request Certificate Modification.....	22
3.	Identification and Authentication	10	4.8.3	Processing Certificate Modification Requests	23
3.1	Naming.....	10	4.8.4	Notification of New Certificate Issuance to Subscriber	23
3.1.1	Type of Names	10	4.8.5	Conduct Constituting Acceptance of Modified Certificate	23
3.1.2	Need for Names to be Meaningful	12	4.8.6	Publication of the Modified Certificate by the CA.....	23
3.1.3	Anonymity or Pseudonymity of Subscribers	12	4.8.7	Notification of Certificate Issuance by the CA to Other Entities.....	23
3.1.4	Rules for Interpreting Various Name Forms	12	4.9	Certificate Revocation and Suspension	23
3.1.5	Uniqueness of Names	12	4.9.1	Circumstances for Revocation	23
3.1.6	Recognition, Authentication, and Role of Trademarks.....	12	4.9.2	Who Can Request Revocation	24
3.2	Initial Identity Validation.....	12	4.9.3	Procedure for Revocation Request	24
3.2.1	Method to Prove Possession of Private Key.....	12	4.9.4	Revocation Request Grace Period.....	25
3.2.2	Authentication of Organization identity	13	4.9.5	Time within Which CA Must Process the Revocation Request	25
3.2.3	Authentication of Individual Identity	13	4.9.6	Revocation Checking Requirements for Relying Parties	25
3.2.4	Non-Verified Subscriber information	14	4.9.7	CRL Issuance Frequency.....	25
3.2.5	Validation of Authority.....	14	4.9.8	Maximum Latency for CRLs	25
3.2.6	Criteria for Interoperation.....	15	4.9.9	On-Line Revocation/Status Checking Availability	25
3.3	Identification and Authentication for Re-key Requests.....	15	4.9.10	On-Line Revocation Checking Requirements	26
3.3.1	Identification and Authentication for Routine Re-key	15	4.9.11	Other Forms of Revocation Advertisements Available	26
3.3.2	Identification and Authentication for Re-key After Revocation	16	4.9.12	Special Requirements regarding Key Compromise	26
3.4	Identification and Authentication for Revocation Request	16	4.9.13	Circumstances for Suspension.....	26
4.	Certificate Life-Cycle Operational Requirements.....	10	4.9.14	Who Can Request Suspension	26
4.1	Certificate Application.....	17	4.9.15	Procedure for Suspension Request.....	26
4.1.1	Who Can Submit a Certificate Application?	17	4.9.16	Limits on Suspension Period.....	27
4.1.2	Enrollment Process and Responsibilities.....	17			
4.2	Certificate Application Processing.....	18			
4.2.1	Performing Identification and Authentication Functions	18			
4.2.2	Approval or Rejection of Certificate Applications.....	18			
4.2.3	Time to Process Certificate Applications	18			
4.3	Certificate Issuance.....	18			
4.3.1	CA Actions during Certificate Issuance.....	18			
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate.....	18			
4.4	Certificate Acceptance	19			
4.4.1	Conduct Constituting Certificate Acceptance.....	19			
4.4.2	Publication of the Certificate by the CA	19			

4.10	Certificate Status Services	27	6.1	Key Pair Generation and Installation	39
4.10.1	Operational Characteristics	27	6.1.1	Key Pair Generation	39
4.10.2	Service Availability	27	6.1.2	Private Key Delivery to Subscriber	40
4.10.3	Optional Features	27	6.1.3	Public Key Delivery to Certificate Issuer	40
4.11	End of Subscription	27	6.1.4	CA Public Key Delivery to Relying Parties	40
4.12	Key Escrow and Recovery	27	6.1.5	Key Sizes	40
4.12.1	Key Escrow and Recovery Policy and Practices	27	6.1.6	Public Key Parameters Generation and Quality	41
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	28	6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)	41
5.	Facility, Management, and Operational Controls	28	6.2	Private Key Protection and Cryptographic Module Engineering Controls	41
5.1	Physical Controls	28	6.2.1	Cryptographic Module Standards and Controls	41
5.1.1	Site Location and Construction	29	6.2.2	Private Key (m out of n) Multi-Person Control	41
5.1.2	Physical Access	29	6.2.3	Private Key Escrow	41
5.1.3	Power and Air Conditioning	29	6.2.4	Private Key Backup	42
5.1.4	Water Exposures	29	6.2.5	Private Key Archival	42
5.1.5	Fire Prevention and Protection	29	6.2.6	Private Key Transfer Into or From a Cryptographic Module	42
5.1.6	Media Storage	30	6.2.7	Private Key Storage on Cryptographic Module	42
5.1.7	Waste Disposal	30	6.2.8	Method of Activating Private Key	42
5.1.8	Off-Site Backup	30	6.2.9	Method of Deactivating Private Key	44
5.2	Procedural Controls	30	6.2.10	Method of Destroying Private Key	44
5.2.1	Trusted Roles	30	6.2.11	Cryptographic Module Rating	44
5.2.2	Number of Persons Required per Task	30	6.3	Other Aspects of Key Pair Management	44
5.2.3	Identification and Authentication for Each Role	31	6.3.1	Public Key Archival	44
5.2.4	Roles Requiring Separation of Duties	31	6.3.2	Certificate Operational Periods and Key Pair Usage Periods	44
5.3	Personnel Controls	31	6.4	Activation Data	46
5.3.1	Qualifications, Experience, and Clearance Requirements	32	6.4.1	Activation Data Generation and Installation	46
5.3.2	Background Check Procedures	32	6.4.2	Activation Data Protection	46
5.3.3	Training Requirements	32	6.4.3	Other Aspects of Activation Data	46
5.3.4	Retraining Frequency and Requirements	33	6.5	Computer Security Controls	47
5.3.5	Job Rotation Frequency and Sequence	33	6.5.1	Specific Computer Security Technical Requirements	47
5.3.6	Sanctions for Unauthorized Actions	33	6.5.2	Computer Security Rating	47
5.3.7	Independent Contractor Requirements	33	6.6	Life Cycle Technical Controls	47
5.3.8	Documentation Supplied to Personnel	33	6.6.1	System Development Controls	47
5.4	Audit Logging Procedures	33	6.6.2	Security Management Controls	47
5.4.1	Types of Events Recorded	33	6.6.3	Life Cycle Security Controls	48
5.4.2	Frequency of Processing Log	34	6.7	Network Security Controls	48
5.4.3	Retention Period for Audit Log	34	6.8	Time-Stamping	48
5.4.4	Protection of Audit Log	34	7.	Certificate, CRL, and OCSP Profiles	48
5.4.5	Audit Log Backup Procedures	34	7.1	Certificate Profile	48
5.4.6	Audit Collection System (Internal vs. External)	34	7.1.1	Version Number(s)	48
5.4.7	Notification to Event-Causing Subject	34	7.1.2	Certificate Extensions	49
5.4.8	Vulnerability Assessments	35	7.1.3	Algorithm Object Identifiers	50
5.5	Records Archival	35	7.1.4	Name Forms	50
5.5.1	Types of Records Archived	35	7.1.5	Name Constraints	51
5.5.2	Retention Period for Archive	35	7.1.6	Certificate Policy Object Identifier	51
5.5.3	Protection of Archive	35	7.1.7	Usage of Policy Constraints Extension	51
5.5.4	Archive Backup Procedures	35	7.1.8	Policy Qualifiers Syntax and Semantics	51
5.5.5	Requirements for Time-Stamping of Records	35	7.1.9	Processing Semantics for the Critical Certificate Policies Extension	51
5.5.6	Archive Collection System (Internal or External)	35	7.2	CRL Profile	51
5.5.7	Procedures to Obtain and Verify Archive Information	36	7.2.1	Version Number(s)	52
5.6	Key Changeover	36	7.2.2	CRL and CRL Entry Extensions	52
5.7	Compromise and Disaster Recovery	36	7.3	OCSP Profile	52
5.7.1	Incident and Compromise Handling Procedures	36	7.3.1	Version Number(s)	52
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	36	7.3.2	OCSP Extensions	52
5.7.3	Entity Private Key Compromise Procedures	36	8.	Compliance Audit and Other Assessments	52
5.7.4	Business Continuity Capabilities after a Disaster	37	8.1	Frequency and Circumstances of Assessment	53
5.8	CA or RA Termination	38	8.2	Identity/Qualifications of Assessor	53
6.	Technical Security Controls	39			

8.3	Assessor's Relationship to Assessed Entity	53	9.6.4	Relying Party Representations and Warranties	58
8.4	Topics Covered by Assessment	53	9.6.5	Representations and Warranties of Other	
8.5	Actions Taken as a Result of Deficiency	53		Participants	58
8.6	Communications of Results	53	9.7	Disclaimers of Warranties	58
9.	Other Business and Legal Matters	54	9.8	Limitations of Liability	58
9.1	Fees	54	9.9	Indemnities	59
9.1.1	Certificate Issuance or Renewal Fees	54	9.9.1	Indemnification by Subscribers	59
9.1.2	Certificate Access Fees	54	9.9.2	Indemnification by Relying Parties	59
9.1.3	Revocation or Status Information Access Fees	54	9.10	Term and Termination	60
9.1.4	Fees for Other Services	54	9.10.1	Term	60
9.1.5	Refund Policy	54	9.10.2	Termination	60
9.2	Financial Responsibility	55	9.10.3	Effect of Termination and Survival	60
9.2.1	Insurance Coverage	55	9.11	Individual Notices and Communications with	
9.2.2	Other Assets	55		Participants	60
9.2.3	Extended Warranty Coverage	55	9.12	Amendments	60
9.3	Confidentiality of Business Information	55	9.12.1	Procedure for Amendment	60
9.3.1	Scope of Confidential Information	55	9.12.2	Notification Mechanism and Period	60
9.3.2	Information Not Within the Scope of Confidential		9.12.3	Circumstances under Which OID Must be	
Information	55	Changed	61
9.3.3	Responsibility to Protect Confidential Information		9.13	Dispute Resolution Provisions	61
.....	55	9.13.1	Disputes among Symantec, Affiliates, and	
9.4	Privacy of Personal Information	56	Customers	61
9.4.1	Privacy Plan	56	9.13.2	Disputes with End-User Subscribers or Relying	
9.4.2	Information Treated as Private	56	Parties	61
9.4.3	Information Not Deemed Private	56	9.14	Governing Law	61
9.4.4	Responsibility to Protect Private Information	56	9.15	Compliance with Applicable Law	62
9.4.5	Notice and Consent to Use Private Information	56	9.16	Miscellaneous Provisions	62
9.4.6	Disclosure Pursuant to Judicial or Administrative		9.16.1	Entire Agreement	62
Process	56	9.16.2	Assignment	62
9.4.7	Other Information Disclosure Circumstances	56	9.16.3	Severability	62
9.5	Intellectual Property rights	56	9.16.4	Enforcement (Attorney's Fees and Waiver of	
9.5.1	Property Rights in Certificates and Revocation		Rights)	62
Information	56	9.16.5	Force Majeure	62
9.5.2	Property Rights in the CPS	57	9.17	Other Provisions	62
9.5.3	Property Rights in Names	57	Appendix A. Table of Acronyms and definitions	63
9.5.4	Property Rights in Keys and Key Material	57	Table of Acronyms	63
9.6	Representations and Warranties	57	Definitions	63
9.6.1	CA Representations and Warranties	57			
9.6.2	RA Representations and Warranties	57			
9.6.3	Subscriber Representations and Warranties	58			

1. INTRODUCTION

This document is the [Certsuperior] Certification Practice Statement (“CPS”). It states the practices that Certsuperior certification authorities (“CAs”) employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the **Symantec Trust Network (STN)** Certificate Policies (“CP”) (see: <https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf>).

The CP is the principal statement of policy governing the STN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STN and providing associated trust services. These requirements, called the “STN Standards,” protect the security and integrity of the STN, apply to all STN Participants, and thereby provide assurances of uniform trust throughout the STN. More information concerning the STN and STN Standards is available in the CP.

Certsuperior has authority over a portion of the STN called its “Sub-domain” of the STN. Certsuperior’s Sub-domain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP sets forth requirements that STN Participants must meet, this CPS describes how Certsuperior meets these requirements within Certsuperior’s Sub-domain of the STN. More specifically, this CPS describes the practices that Certsuperior employs for:

- securely managing the core infrastructure that supports the STN, and
- issuing, managing, revoking, and renewing STN Certificates

within Certsuperior’s Sub-domain of the STN, in accordance with the requirements of the CP and its STN Standards.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction. CAs within the Symantec Trust Network hierarchy conform to the current version of the CA/Browser Forum (CABF) requirements including:

- Guidelines for the Issuance and Management of Extended Validation (EV) Certificates,
- Guidelines for the Issuance and Management of Extended Validation (EV) Code-Signing Certificates, and,
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

published at www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.

At this time, Symantec’s Extended Validation (EV) SSL certificates, Extended Validation (EV) Code-Signing certificates and Domain-Validated (DV) and Organization-Validated (OV) SSL Certificates issued by Symantec CAs under this CP conform with the CABF Requirements. Such DV and OV certificates are issued containing the corresponding policy identifier(s) specified in section 1.2 of the CP indicating adherence to and conformance with these requirements. Symantec CAs assert that all Certificates issued containing these policy identifier(s) are issued and managed in conformance with the CABF Requirements.

Effective February 1, 2017 and after, the STN adopts the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <https://aka.ms/csbr>. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Code signing certificates issued on or after February 1st, 2017 and intended for use in Microsoft Authenticode and subsequent technologies will include the applicable certificate policy identifier, 2.23.140.1.4.1, to indicate compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

1.1 Overview

Service Center: Certsuperior is a Service Center as described in CP §1.1.2.1.2 which means Certsuperior can approve or reject Certificate Applications in the case of Retail Certificates or, in the case of Enterprise Certificates, arrange with a Processing Center to provide Enterprise Customers with back-end Certificate lifecycle services. Service Center Affiliates providing client Certificates (“Client Service Centers”) become CAs within the STN but outsource back-end functions to Symantec or another Processing Center. When providing server Certificates, however, Service Centers become RAs within the STN for a Symantec CA issuing server certificates. These Service Centers (“Service Centers”) perform validation functions to approve or reject Certificate applications for Secure Server IDs or Global Server IDs. Service Centers can also provide Managed PKI to their Enterprise Customers. These Managed PKI Customers enter into a Managed PKI arrangement with the Service Center, which under its contract with Certsuperior or another Processing Center, arranges to have the Processing Center provide back-end Certificate lifecycle services to these Managed PKI Customers.

This CPS is specifically applicable to:

-

- Symantec's Public Primary Certification Authorities (PCAs),
- Certsuperior Infrastructure CAs, and Certsuperior Administrative CAs supporting the Symantec Trust Network
- Certsuperior's Public CAs and the CAs of enterprise Customers, who issue Certificates within Certsuperior's sub-domain of the STN.

More generally, the CPS also governs the use of STN services within Certsuperior's Sub-domain of the STN by all individuals and entities within Certsuperior's Sub-domain (collectively, Certsuperior Sub-domain Participants"). Private CAs and hierarchies managed by Certsuperior are outside the scope of this CPS.

The STN includes four classes of Certificates, Classes 1-4. The CP is a single document that defines these certificate policies, one for each of the Classes, and sets STN Standards for each Class.

Certsuperior offers three Classes of Certificates within its Sub-domain of the STN. This CPS describes how Certsuperior meets the CP requirements for each Class within its Sub-domain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all three Certificate Classes.

Certsuperior may publish Certificate Practices Statements that are supplemental to this CPS in order to comply with the specific policy requirements of Government, or other industry standards and requirements.

These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

The CPS is only one of a set of documents relevant to Certsuperior's Sub-domain of the STN. These other documents include:

- Ancillary confidential security and operational documents¹ that supplement the CP and CPS by providing more detailed requirements, such as:
 - The Symantec Physical Security Policy, which sets forth security principles governing the STN infrastructure,
 - The Symantec Security and Audit Requirements (SAR) Guide, which describes detailed requirements for Symantec and Affiliates concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
 - Key Ceremony Reference Guide, which presents detailed key management operational requirements.
- Ancillary agreements imposed by Certsuperior. These agreements bind Customers, Subscribers, and Relying Parties of Certsuperior. Among other things, the agreements flow down STN Standards to these STN Participants and, in some cases, state specific practices for how they must meet STN Standards.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing STN Standards where including the specifics in the CPS could compromise the security of Certsuperior's Sub-domain of the STN.

1.2 Document name and Identification

This document is the Certsuperior Certification Practice Statement. STN Certificates contain object identifier values corresponding to the applicable STN Class of Certificate. Therefore, Certsuperior has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with [Section 7.1.6](#).

Domain validated and organization validated SSL Certificates contain the corresponding OID value in section 1.2 of the STN CP that indicates adherence to and compliance with the CA / Browser Forum Baseline Requirements (see STN CP detail at: <https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf>).

Extract from STN CP (<https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf>) regarding Document Name and Identification:

1.2 Document Name and Identification

This document is the Symantec Trust Network (STN) Certificate Policy (CP). Symantec, acting as the policy-defining authority, has assigned an object identifier (OID) value extension for each Class of Certificate issued under the Symantec Trust Network (STN). The object identifier values used for the Classes of end-user Subscriber Certificates are:

- The Class 1 Certificate Policy: Symantec/pki/policies/stn-cp/class1 (2.16.840.1.113733.1.7.23.1).
- The Class 2 Certificate Policy: Symantec/pki/policies/stn-cp/class2 (2.16.840.1.113733.1.7.23.2).
- The Class 3 Certificate Policy: Symantec/pki/policies/stn-cp/class3 (2.16.840.1.113733.1.7.23.3)
- The Class 3 Certificate Policy for Symantec Private Hierarchy: Symantec/pki/policies/stn-cp/class3 (2.16.840.1.113733.1.7.23.3.2)
- The Class 3 EV Certificate Policy: Symantec/pki/stn-cp/Class3/Enhanced validation (2.16.840.1.113733.1.7.23.6)

The "Class 3 Certificate Policy for Symantec Private Hierarchy" adopts in its entirety the Class 3 policy defined by this CP with the exception that the hierarchy is limited to Symantec Internal CAs and the Primary Certification Authority (PCA) certificate shall not be added to public certificate trust lists.

Each OID above may be extended further to define additional policies covering a particular type

¹ Although these documents are not publicly available their specifications are included in Symantec's Annual WebTrust for Certification authorities audit and may be made available to customer under special Agreement

of certificate. The extended OID shall be defined in the particular CPS for that product. For example, a Non-Federal SSP certificate issued under the STN at the Basic level has a Class 2 OID defined in the Symantec Non-Federal SSP CPS as follows, 2.16.840.1.113733.1.7.23.2.1.1 and at the Medium level has a Class 3 OID defined as 2.16.840.1.113733.1.7.23.3.1.1.

1.2.1 CABF Policy Identifiers

Symantec has assigned a reserved OID value for asserting conformance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates. This OID value is reserved for use by any brand of Symantec CA as a means of asserting compliance with these CABF Requirements and as such does not distinguish a particular brand or class of Certificate.

- The Symantec Reserved Certificate Policy identifier: Symantec/id-CABF-OVandDVvalidation (2.16.840.1.113733.1.7.54)
- For certificate key sizes smaller than 2048 bit will use the object identifier value of (2.16.840.1.113733.1.8.54.1)

Most DV and OV certificates issued on or after March 5th, 2015 will include the applicable CABF policy OIDs:

- CABF OID for DV certificates: 2.23.140.1.2.1
- CABF OID for OV certificates: 2.23.140.1.2.2

All DV and OV certificates issued after May 2015 will include the applicable CABF policy OIDs.

1.2.2 Microsoft Policy Identifiers

Code signing certificates issued on or after February 1st, 2017 will include the applicable certificate policy identifier, 2.23.140.1.4.1, to indicate compliance with the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

1.3 PKI Participants

1.3.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the STN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots of four domains², one for each class of Certificate. Each PCA is a Symantec entity. Subordinate to the PCAs are Certsuperior Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

Symantec also operates the “Symantec Universal Root Certification Authority” and the “Symantec ECC Universal Root Certification Authority”. The Universal Root CAs are not defined under a particular certificate Class, and may issue any class of Subordinate CA.

Certsuperior enterprise customers may operate their own CAs as a subordinate CA to a Certsuperior PCA. Such a customer enters into a contractual relationship with Certsuperior to abide by all the requirements of the STN CP and the Certsuperior CPS. These subordinate CAs may, however implement a more restrictive practices based on their internal requirements.

One STN CA technically outside the three hierarchies under each of the PCAs is the Secure Server Certification Authority. This CA does not have a superior CA, such as a root or a PCA. Rather, the Secure Server CA acts as its own root and has issued itself a self-signed root Certificate. It also issues Certificates to end-user Subscribers. Thus, the Secure Server Hierarchy consists only of the Secure Server CA. The Secure Server CA issues Secure Server IDs, which are deemed to be Class 3 Organizational Certificates.

² Class 4 certificates are not currently issued by the STN

The Secure Server CA employs lifecycle practices that are substantially similar with those of other Class 3 CAs within the STN. Thus, Symantec has approved and designated the Secure Server Certification Authority as a Class 3 CA within the STN. The Certificates it issues are considered to provide assurances of trustworthiness comparable to other Class 3 organizational Certificates.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a STN CA. Certsuperior may act as an RA for certificates it issues with the exception of EV and Code-Signing Certificates. Symantec Corporations shall act as the RA for all Certificate Requests for EV and Code-Signing Certificates issued by Certsuperior.

Third parties, who enter into a contractual relationship with Certsuperior, may operate their own RA and authorize the issuance of certificates by a Certsuperior CA. Third party RAs must abide by all the requirements of the STN CP, the Certsuperior CPS and the terms of their enterprise services agreement with Certsuperior. RAs may, however implement more restrictive practices based on their internal requirements.³

1.3.3 Subscribers

Subscribers under the STN include all end users (including entities) of certificates issued by a STN CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with Certsuperior for the issuance of credentials and; "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When 'Subject' is used, it is to indicate a distinction from the Subscriber. When "Subscriber" is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within the STN, either as a PCA issuing a self signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under the STN. A Relying party may, or may not also be a Subscriber within the STN.

³ An example of a third party RA is a customer of Managed PKI services customer.

1.3.5 Other Participants

Not applicable

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

1.4.1.1. Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for individual certificates are included in Table 1 below, an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the STN CP, the CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	Assurance Level			Usage		
	Low assurance level	Medium assurance level	High assurance Level	Signing	Encryption	Client Authentication
Class 1 Certificates	✓			✓	✓	✓
Class 2 Certificates		✓		✓	✓	✓
Class 3 Certificates			✓	✓	✓	✓

Table 1. Individual Certificate Usage

1.4.1.2 Certificates issued to Organizations

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. It is not the intent of this CPS to limit the types of usages for Organizational Certificates. While the most common usages are included in Table 2 below, an organizational certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by the STN CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	Assurance Level		Usage			
	High assurance level	Medium assurance level	Code/Content Signing	Secure SSL/TLS-sessions	Authentication	Signing and encryption
Class 3 Certificates	✓		✓	✓	✓	✓

Table 2. Organizational Certificate Usage⁴

⁴ "In limited circumstances Class 2 certificates may be issued by a Managed MPKI customer to an affiliated organization (and not an individual within the organization). Such certificate may be used for organization authentication and application signing only. Except as expressly authorized by Symantec through an Enterprise Service Agreement imposing authentication and practice requirements consistent with the security standards of this CPS, Subscribers are prohibited from using this certificate for code and content signing, SSL encryption and S/mime signing and such key usage will be disabled for these certificates."

1.4.1.3 Assurance levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity, in relation to Class 1 and 3.

High assurance Certificates are individual and organizational certificates Class 3 Certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2.

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

Symantec and Certsuperior Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, Class 1 Certificates shall not be used as proof of identity or as support of non repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

Symantec and Certsuperior periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. Certsuperior therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. Certsuperior recommends the use of PCA Roots as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Certsuperior
Av. Santa Fe # 170 Of. 3-2-06, Col. Lomas de Santa Fe.
Del Alvaro Obregon, Mexico, D.F., C.P. 01210
Attn: Practices Development – CPS
Certsuperior phone number
Phone: +52(55)59855000
Fax: +52(55)50814376
practices@Certsuperior.com

1.5.2 Contact Person

The Certificate Policy Manager
Symantec Trust Network Policy Management Authority
c/o Certsuperior
Av. Santa Fe # 170 Of. 3-2-06, Col. Lomas de Santa Fe.
Del Alvaro Obregon, Mexico, D.F., C.P. 01210
Attn: Practices Development – CPS
Certsuperior phone number
Phone: +52(55)59855000
Fax: +52(55)50814376
practices@Certsuperior.com

1.5.3 Person Determining CP Suitability for the Policy

The organization identified in Section 1.5.2 is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the CP and this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments shall be made by the PMA. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be linked to the Practices Updates and Notices section of the Certsuperior Repository located at:

<https://www.Certsuperior.com/repository/updates>. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions

2. Publication and Repository Responsibilities

2.1 Repositories

Certsuperior is responsible for the repository functions for its own CAs and the CAs of its Enterprise Customers (either Managed PKI or ASB customers). Certsuperior issuing Certificates to end-user Subscribers publish Certificates they issue in the repository in accordance with CPS § 2.6.

Upon revocation of an end-user Subscriber's Certificate, Certsuperior publishes notice of such revocation in the repository. Certsuperior issues CRLs for its own CAs and the CAs of Service Centers and Enterprise Customers within its Sub-domain, pursuant to the provisions of this CPS. In addition, Enterprise Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, Certsuperior provides OCSP services pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

Certsuperior maintains a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. Time or Frequency of Publication (this is not a heading)

Updates to this CPS are published in accordance Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

Certsuperior publishes the Certificates it issues on behalf of its own CAs, and the CAs of Client Service Centers in their Sub-domain. Upon revocation of an end-user Subscriber's Certificate, Certsuperior shall publish notice of such revocation in the repository. In addition, Certsuperior issues Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs of Service Centers within its Sub-domain.

Certsuperior will at all times publish a current version of:

- o The STN CP
- o The Certsuperior CPS,
- o Subscriber Agreements,
- o Relying Party Agreements

Certsuperior is responsible for the repository function for Certsuperior CAs and Enterprise Customers' CAs that issue Certificates within Certsuperior's Sub-domain of the STN.

Certsuperior publishes certain CA information in the repository section of Certsuperior's web site at <http://www.certsuperior.com/repository/> as described below.

Certsuperior publishes the STN CP, this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of Certsuperior's web site.

Certsuperior publishes Certificates in accordance with Table 3 below.

Certificate Type	Publication Requirements
STN PCA and STN Issuing Root CA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Certsuperior Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Certificate of the Certsuperior CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the Certsuperior LDAP directory server at <i>directory. Certsuperior.com</i> .
Symantec OCSP Responder Certificates	Available through query of the Certsuperior LDAP directory server at <i>directory. Certsuperior.com</i> .
End-User Subscriber Certificates with exceptions for certain Class 3 Certificates depending on usage.	Optionally published and available to relying parties through query functions in the Certsuperior repository at: https://www.Certsuperior.com/repository and query of the Symantec LDAP directory server at <i>directory.verisign.com</i> except for Class 3 SSL and Code Signing Certificates which are available through query functions in the Certsuperior repository at: https://www.Certsuperior.com/repository .

Certificate Type	Publication Requirements
End-User Subscriber Certificates issued through Managed PKI Customers	Made available through the query functions listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.

Table 3 – Certificate Publication Requirements

2.3 Frequency of Publication

Updates to this CPS are published in accordance Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

2.4 Access Controls on Repositories

Information published in the repository portion of the Certsuperior web site is publicly-accessible information. Read only access to such information is unrestricted. Certsuperior requires persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. Certsuperior has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

3.1 Naming

Unless where indicated otherwise in the STN CP, this CPS or the content of the digital certificate, names appearing in Certificates issued under STN are authenticated.

3.1.1 Type of Names

While the STN is currently owned by Symantec Corporation, legacy certificates have been issued in the name of the former owner. Any legacy certificate that indicates the Organization (O) as "VeriSign, Inc." and Organizational Unit (OU) as "VeriSign Trust Network" shall mean Symantec Corporation and the Symantec Trust Network, respectively.

Certsuperior CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. Certsuperior CA Distinguished Names consist of the components specified in Table 4 below.

Attribute	Value
Country (C) =	"MX", "US" or not used.
Organization (O) =	"Symantec Corporation" or Certsuperior ⁵ or <organization name> ⁶
Organizational Unit (OU) =	Certsuperior CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: <ul style="list-style-type: none"> • CA Name • Symantec Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and • A copyright notice. • Text to describe the type of Certificate.
State or Province (S) =	Not used.

⁵ An exception to this is the Secure Server CA, which indicates "RSA Data Security, Inc.," but is now a Symantec CA.

⁶ For a CA dedicated to a customer organization, the (o=) component shall be the legal name of the organization.

Attribute	Value
Locality (L) =	Not used except for the Symantec Commercial Software Publishers CA, which uses "Internet."
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.

Table 4 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 5 below.

Attribute	Value
Country (C) =	"MX" or not used
Organization (O) =	The Organization attribute is used as follows: <ul style="list-style-type: none"> • "Certsuperior" for Certsuperior OCSP Responder and optionally for individual Certificates that do not have an organization affiliation. • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation.
Organizational Unit (OU) =	Certsuperior end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: <ul style="list-style-type: none"> • Subscriber organizational unit (for organizational Certificates and individual Certificates that have an organization affiliation) • Symantec Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Certsuperior" and "Member, Symantec Trust Network" in Certificates whose applications were authenticated by Symantec • "Persona Not Validated" for Class 1 Individual Certificates • Text to describe the type of Certificate. • "No organization affiliation" (for code signing certificates issued to individuals)
State or Province (S) =	Indicates the Subscriber's State or Province (State is not a required field in certificates issued to individuals).
Locality (L) =	Indicates the Subscriber's Locality (Locality is not a required field in certificates issued to individuals).
Common Name (CN) =	This attribute includes: <ul style="list-style-type: none"> • The OCSP Responder Name (for OCSP Responder Certificates) • Domain name (for web server Certificates) • Organization name (for code/object signing Certificates) • Person's name (for individual Certificates or code-signing certificates issued to individuals).
E-Mail Address (E) =	E-mail address for Class 1 individual Certificates and generally for MPKI Subscriber Certificates

Table 5 – Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Class 2-3 Certificates.

- The authenticated common name value included in the Subject distinguished names of organizational Certificates is a domain name (in the case of Secure Server IDs and Global Server IDs) or the legal name of the organization or unit within the organization.

- The authenticated common name value included in the Subject distinguished name of a Class 3 Organizational ASB Certificate, however, is the generally accepted personal name of the organizational representative authorized to use the organization's private key, and the organization (O=) component is the legal name of the organization.
- The common name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

Class 2 and 3 end-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

Certsuperior CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The identity of Class 1 individual Subscribers is not authenticated. Class 1 subscribers may use pseudonyms. Unless when required by law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g., minors, or sensitive government employee information), Class 2 and 3 Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by the PMA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

Certsuperior ensures that Subject Distinguished Names of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Certsuperior, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. Certsuperior is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall

be PKCS #10, another cryptographically equivalent demonstration, or another Certsuperior - approved and Symantec-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization identity

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in Certsuperior's documented Validation Procedures.

At a minimum Certsuperior shall:

- determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization,
- confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

Where a domain name or e-mail address is included in the certificate Certsuperior authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain.

Additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science ("BIS") are performed by Certsuperior when required.

Additional procedures are performed for specific types of Certificates as described in Table 6 below.

Certificate Type	Additional Procedures
Managed PKI for Intranet SSL Certificate	Symantec verifies that the host name or IP address assigned to a Device is not accessible from the Internet (publicly facing), and is owned by the Certificate Subscriber.
Authenticated Content Signing Certificate	Before Symantec digitally signs any content using ACS it authenticates that the content is the original content signed by the Organization using its Code Signing Certificate.

Table 6. Specific Authentication Procedures

3.2.3 Authentication of Individual Identity

Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of STN certificate is explained in Table 7 below.

Certificate Class	Authentication of Identity
Class 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.

Certificate Class	Authentication of Identity
Class 2	<p>Authenticate identity by matching the identity provided by the Subscriber to:</p> <ul style="list-style-type: none"> ○ information residing in the database of a Certsuperior -approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or ○ information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals
Class 3	<p>The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of the CA or RA, or before a notary public or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognized form of government-issued photographic identification, such as a passport or driver's license and one other identification credential.</p> <p>The authentication of Class 3 Administrator certificates is based on authentication of the organization and a confirmation from the organization of the identity and authorization of the person to act as Administrator.</p> <p>Certsuperior may also have occasion to approve Certificate Applications for their own Administrators. Administrators are "Trusted Persons" within an organization. In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.⁷</p>

Table 7. Authentication of individual identity

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU)
- Subscriber's name in Class 1 certificates
- Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization Certsuperior or a RA:

- determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

⁷ Certsuperior may approve Administrator Certificates to be associated with a non-human recipient such as a device, or a server. Authentication of a Class 3 Administrator Certificate Applications for a non-human recipient shall include:

- Authentication of the existence and identity of the service named as the Administrator in the Certificate Application
- Authentication that the service has been securely implemented in a manner consistent with it performing an Administrative function
- Confirmation of the identity and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

3.2.6 Criteria for Interoperation

Certsuperior may provide interoperation services that allow a non-STN CA to be able to interoperate with the STN by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with the STN CP as supplemented by additional policies when required.

Certsuperior shall only allow interoperation with the STN of a non-STN CA in circumstances where the CA, at a minimum:

- Enters into a contractual agreement with Certsuperior
- Operates under a CPS that meets STN requirements for the classes of certificates it will issue
- Passes a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

3.3 *Identification and Authentication for Re-key Requests*

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. Certsuperior generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey") However, in certain cases (i.e., for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of Certsuperior Certificates, except for Class 3 Server Certificates, this distinction is not important as a new key pair is always generated as part of Certsuperior's end-user Subscriber Certificate replacement process. However, for Class 3 Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal."

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) Symantec may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, Symantec will issue the Certificate if the enrollment information (including Corporate and Technical contact information⁸) has not changed.

⁸ If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, Certsuperior or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.⁹

In particular, for retail Class 3 Organizational certificates through www.certsuperior.com, Certsuperior re-authenticates the Organization name and domain name included in the certificate at intervals described in section 6.3.2. In circumstances where:

- The challenge phrase is correctly used for the subsequent renewal certificate and;
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

Certsuperior will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

Rekey after 30-days from expiration of the Certificate are re-authenticated as an original Certificate Application and are not automatically issued.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or
- the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or
- the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.
- For any other reason deemed necessary by Symantec or Certsuperior to protect the STN

Subject to the foregoing paragraph, renewal of an organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the organization or CA seeking renewal is in fact the Subscriber of the Certificate. Renewed organizational Certificates shall contain the same Subject distinguished name as the Subject distinguished name of the organizational Certificate being renewed.

Renewal of an individual Certificate following revocation must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another Certsuperior-approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, Certsuperior verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

⁹ The authentication of a request to rekey/renew a Class 3 Organizational ASB Certificate, however, requires the use of a Challenge Phrase as well as the same identification and authentication as for the original Certificate Application.

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option may not be available to all customers.)
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

Certsuperior Administrators are entitled to request the revocation of end-user Subscriber Certificates within Certsuperior's Sub domain. Certsuperior authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another STN-approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to Certsuperior. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

The requests to revoke a CA Certificate shall be authenticated by the Certsuperior to ensure that the revocation has in fact been requested by the CA.

4. Certificate Life-Cycle Operational Requirements

4.1 *Certificate Application*

4.1.1 Who Can Submit a Certificate Application?

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to Certsuperior
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to Certsuperior.

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with Certsuperior. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate

with Certsuperior to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 *Certificate Application Processing*

4.2.1 Performing Identification and Authentication Functions

Certsuperior or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.2.2 Approval or Rejection of Certificate Applications

Certsuperior or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received

Certsuperior or an RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the STN into disrepute.

4.2.3 Time to Process Certificate Applications

Certsuperior begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between STN participants. A certificate application remains active until rejected.

4.3 *Certificate Issuance*

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by Certsuperior or following receipt of an RA's request to issue the Certificate. Certsuperior creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Certsuperior shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

Certsuperior publishes the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber agreement and accepted the certificate. The certificate shall be used lawfully in accordance with Certsuperior's Subscriber Agreement the terms of the STN CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. Certsuperior is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is

reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate. Certificate renewal is supported for Class 3 certificates where the key pair is generated on a web server as most web server key generation tools permit the creation of a new Certificate Request for an existing key pair.

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew a new certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration.

4.6.2 Who May Request Renewal

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal.

4.6.3 Processing Certificate Renewal Requests

Renewal procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information¹⁰) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) Certsuperior may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, Certsuperior will issue the Certificate if the enrollment information (including corporate and technical contact information¹¹) has not changed.

After renewal in this fashion, and on at least alternative instances of subsequent renewal thereafter, Certsuperior or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

¹⁰ If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

¹¹ If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

In particular, for retail Class 3 Organizational certificates through www.certsuperior.com, Certsuperior re-authenticates the Organization name and domain name included in the certificate at intervals described in section 6.3.2. In circumstances where:

- The challenge phrase is correctly used for the subsequent renewal certificate and;
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

Certsuperior will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

Other than this procedure or another Certsuperior -approved procedure, the requirements for the authentication of an original Certificate Application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed certificate is in accordance with Section 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in Certsuperior's publicly accessible repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.7 *Certificate Re-Key*

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all certificate Classes.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information¹²) has not changed, a renewal Certificate is automatically issued. Subject to the provisions of Section 3.3.1, after re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, Certsuperior or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

Other than this procedure or another Symantec-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in Certsuperior's publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

¹² If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

4.8.3 Processing Certificate Modification Requests

Certsuperior or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 *Certificate Revocation and Suspension*

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by Symantec (or by the Subscriber) and published on a CRL. Upon request from a subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, Symantec will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- Certsuperior, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- Certsuperior or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- The affiliation between an organization that is a Subscriber of a Class 3 Organizational ASB Certificate and the organizational representative controlling the Subscriber's private key is terminated or has otherwise ended,
- Certsuperior or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the Subject of such Certificate,
- Certsuperior or a Customer has reason to believe that a material fact in the Certificate Application is false,
- Certsuperior or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,

- In the case of Class 3 organizational Certificates, the Subscriber's organization name changes,
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed,
- The Subscriber identity has not been successfully re-verified in accordance with section 6.3.2,
- The Subscriber has not submitted payment when due, or
- The continued use of that certificate is harmful to the STN.

When considering whether certificate usage is harmful to the STN, Certsuperior considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

When considering whether the use of a Code Signing Certificate is harmful to the STN, Certsuperior additionally considers, among other things, the following:

- The name of the code being signed
- The behavior of the code
- Methods of distributing the code
- Disclosures made to recipients of the code
- Any additional allegations made about the code

Certsuperior may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

Certsuperior Subscriber Agreements require end-user Subscribers to immediately notify Certsuperior of a known or suspected compromise of its private key.

4.9.2 Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of Certsuperior or an RA. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of Certsuperior or a RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only Certsuperior is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to the Certsuperior or the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. For Enterprise customers, the Subscriber is required to communicate the request to the Enterprise Administrator who will communicate the revocation

request to Certsuperior for processing. Communication of such revocation request shall be in accordance with CPS § 3.4.

Where an Enterprise Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer or ASB Customer instructs Certsuperior to revoke the Certificate.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to Certsuperior. Certsuperior will then revoke the Certificate. Certsuperior may also initiate CA or RA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

Certsuperior takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but also whenever a CA Certificate is revoked.

CRLs for Authenticated Content Signing (ACS) Root CAs are published annually and also whenever a CA Certificate is revoked.

If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. In addition to publishing CRLs, Certsuperior provides Certificate status information through query functions in the Certsuperior repository.

Certificate status information is available through web-based query functions accessible through the Certsuperior Repository at

- <https://www.Certsuperior.com/repository> (for SSL and Code Signing Certificates).

Certsuperior also provides OCSP Certificate status information. Enterprise Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Enterprise Customer.

4.9.10 On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements regarding Key Compromise

Certsuperior uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their sub-domains.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

4.9.17 Not applicable.Circumstances for Suspension

Not applicable.

4.9.18 Who Can Request Suspension

Not applicable.

4.9.19 Procedure for Suspension Request

Not applicable.

4.9.20 Limits on Suspension Period

Not applicable.

4.10 *Certificate Status Services*

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at Certsuperior's website, LDAP directory and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24x7 without scheduled interruption.

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products.

4.11 *End of Subscription*

A subscriber may end a subscription for a Certsuperior certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 *Key Escrow and Recovery*

With the exception of enterprises deploying Managed PKI Key Management Services no STN participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using Managed PKI Key Management Service (KMS) can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. The enterprise customer may use KMS operated either out of the enterprise's premises or [Affiliate's] secure data center. If operated out of the enterprise's premises, Certsuperior does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Managed PKI Key Management service (or an equivalent service approved by Symantec) are permitted to escrow end-user Subscribers' private key. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by Symantec), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,

- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that Enterprise Customers using KMS:

- Notify the subscribers that their private keys are escrowed
- Protect subscribers' escrowed keys from unauthorized disclosure,
- Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys.
- Release subscribers' escrowed keys only for properly authenticated and authorized requests for recovery.
- Revoke the Subscriber's Key pair prior to recovering the encryption key under certain circumstances such as to discontinue the use of a lost certificate.
- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.
- Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored in the Key Manager database in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER) is generated, then the triple-DES key is combined with a random session key to form a session key mask. The resulting masked session key (MSK) is securely sent and stored in the Managed PKI database at Certsuperior. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database and all residual key material is destroyed.

The Managed PKI database is operated out of Certsuperior's secure data center. The enterprise customer may choose to operate the Key Manager database either on the enterprise's premises or out of Certsuperior's secure data center.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database. The Key Manager retrieves the session key from the KMD and combines it with the MSK to regenerate the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

5. Facility, Management, and Operational Controls

5.1 *Physical Controls*

Certsuperior has implemented the Certsuperior Physical Security Policy, which supports the security requirements of this CPS. Compliance with these policies is included in Certsuperior's independent audit requirements described in Section 8. The Certsuperior Physical Security Policy

contains sensitive security information and is only available upon agreement with Certsuperior. An overview of the requirements are described below.

5.1.1 Site Location and Construction

Certsuperior CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

Certsuperior also maintains disaster recovery facilities for its CA operations. Certsuperior's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of Certsuperior's primary facility.

5.1.2 Physical Access

Certsuperior CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with Certsuperior's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

Certsuperior's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

Certsuperior has taken reasonable precautions to minimize the impact of water exposure to Certsuperior systems.

5.1.5 Fire Prevention and Protection

Certsuperior has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. Certsuperior's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within Certsuperior facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with Certsuperior's normal waste disposal requirements.

5.1.8 Off-Site Backup

Certsuperior performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and Certsuperior's disaster recovery facility.

5.2 *Procedural Controls*

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

Certsuperior considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

Certsuperior has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA

cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold "Secret Shares" and vice versa.

Other manual operations such as the validation and issuance of Class 3 Certificates, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing Symantec HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

Certsuperior ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on STN CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to)

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, recovery requests or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

Certsuperior requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, Certsuperior conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, Certsuperior will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavorable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

Certsuperior provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. Certsuperior maintains records of such training. Certsuperior periodically reviews and enhances its training programs as necessary.

Certsuperior's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- Certsuperior security and operational policies and procedures,
- Use and operation of deployed hardware and software,

- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

Certsuperior provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

Not applicable

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of Certsuperior policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to an Certsuperior employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to Certsuperior's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

Certsuperior provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 *Audit Logging Procedures*

5.4.1 Types of Events Recorded

Certsuperior manually or automatically logs the following significant events:

- CA key life cycle management events, including:
 - Key generation, backup, storage, recovery, archival, and destruction
 - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
 - Certificate Applications, renewal, rekey, and revocation
 - Successful or unsuccessful processing of requests
 - Generation and issuance of Certificates and CRLs.
- Security-related events including:
 - Successful and unsuccessful PKI system access attempts
 - PKI and security system actions performed by Certsuperior personnel
 - Security sensitive files or records read, written or deleted
 - Security profile changes
 - System crashes, hardware failures and other anomalies
 - Firewall and router activity

- CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

Certsuperior RAs and Enterprise Administrators log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's drivers license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, Certsuperior reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within Certsuperior CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by Certsuperior personnel.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments (“LSVAs”) are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity’s annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

Certsuperior archives:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked.

- Five (5) years for Class 1 Certificates,
- Ten (10) years and six (6) months for Class 2 and Class 3 Certificates

5.5.3 Protection of Archive

Certsuperior protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

Certsuperior incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

Certsuperior archive collection systems are internal, except for enterprise RA Customers. Certsuperior assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

Certsuperior CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. Certsuperior CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). Certsuperior's CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. Certsuperior maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Sub-domain.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Certsuperior Security and Certsuperior's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Certsuperior's key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of an Certsuperior CA, STN infrastructure or Customer CA private key, Certsuperior's Key Compromise Response procedures are enacted by the Certsuperior Security Incident Response Team (ASSIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other Symantec management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from Certsuperior executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the Certsuperior Repository in accordance with CPS § 4.9.7,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected STN Participants, and
- The CA will generate a new key pair in accordance with CPS § 5.6, except where the CA is being terminated in accordance with CPS § 5.8.

5.7.4 Business Continuity Capabilities after a Disaster

Symantec has implemented a disaster recovery site more than 1000 miles from Symantec's principal secure facilities. Symantec has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. Symantec's disaster recovery site has implemented the physical security protections and operational controls required by the Symantec Security and Audit Requirements (SAR) Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from Symantec's primary facility, Symantec's disaster recovery process is initiated by the Symantec Emergency Response Team (SERT).

Symantec has the capability to restore or recover essential operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- publication of revocation information, and
- provision of key recovery information for Enterprise Customers using Managed PKI Key Manager.

Symantec's disaster recovery database is synchronized regularly with the production database within the time limits set forth in the Security and Audit Requirements Guide. Symantec's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

Symantec's disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at Symantec's primary site. Symantec tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at Symantec's primary site as soon as possible following a major disaster.

Symantec maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4.

Symantec maintains offsite backups of important CA information for Symantec CAs as well as the CAs of Service Centers, and Enterprise Customers, within Symantec's Sub-domain. Such information includes, but is not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

Certsuperior

For services where the entity issuing Certificates is Certsuperior (see CPS §1.1.2.1.2), Certsuperior has implemented a disaster recovery site more than 1,000 miles from Certsuperior's principal secure facilities. Certsuperior has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. Certsuperior's disaster recovery site has implemented the physical security protections and operational controls required by the Symantec Security and Audit Requirements (SAR) Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from Certsuperior's primary facility, Certsuperior's disaster recovery process is initiated by the Certsuperior Emergency Response Team (ASERT).

Certsuperior has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- publication of revocation information, and
- provision of key recovery information for Managed PKI Customers using Managed PKI Key Manager.

Certsuperior's disaster recovery database is synchronized regularly with the production database within the time limits set forth in the SAR Guide. Certsuperior's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

Certsuperior's disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at Certsuperior's primary site. Certsuperior tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at Certsuperior's primary site as soon as possible following a major disaster.

Certsuperior maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4.

Certsuperior maintains offsite backups of important CA information for Certsuperior CAs as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within Certsuperior's Subdomain. Such information includes, but is not limited to: application logs, Certificate Application data, audit data (per CPS § 4.5), and database records for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary for a Certsuperior CA, or Enterprise Customer CA to cease operation, Certsuperior makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, Certsuperior and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by Certsuperior,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

6. Technical Security Controls

6.1 *Key Pair Generation and Installation*

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3. For other CAs (including Certsuperior CAs and Managed PKI Customer CAs), the cryptographic modules used meet the requirements of at least FIPS 140-1 level 2.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the Symantec SAR Guide. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Certsuperior Management.

Generation of RA key pairs is generally performed by the RA using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Enterprise Customers generate the key pair used by their Automated Administration servers. Certsuperior recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Class 1 Certificates, Class 2 Certificates, and Class 3 code/object signing Certificates, the Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

For ACS Application IDs, Certsuperior generates a key pair on behalf of the Subscriber using a random numbers seed generated on a cryptographic module that, at a minimum, meets the requirements of FIPS 140-1 level 3.

6.1.2 Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable. For ACS Application IDs, private key delivery to a Subscriber is also not applicable.

Where RA or end-user Subscriber key pairs are pre-generated by Certsuperior on hardware tokens or smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by Certsuperior.

Where end-user Subscriber key pairs are pre-generated by Enterprise Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Enterprise Customer.

For Enterprise Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS # 12 file.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to Symantec for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by Symantec, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

Certsuperior makes the CA Certificates for Symantec PCAs and its root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, Certsuperior provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

Certsuperior generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. Certsuperior CA Certificates may also be downloaded from the Certsuperior LDAP Directory at *directory.Certsuperior.com*.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The Certsuperior Standard for minimum key sizes is the use of key pairs equivalent in strength to 2048 bit RSA for PCAs and CAs¹³.

Symantec's third and fifth generation (G3 and G5) PCAs have 2048 bit RSA key pairs.

¹³ CA trust is extended to Symantec's first and second generation (G1 and G2) legacy Trusted Roots with 1024 bit RSA key pairs for support of customer legacy platforms and 1024-bit RSA end-entity certificates may be issued with expiration on or before December 31, 2011. Additional individual exceptions may be permitted with prior approval to preserve business continuity of legacy applications beyond 2011.

Symantec issues minimum key size equivalent in strength to 2048 bit RSA for RAs and end entity certificates key pairs.

Symantec's fourth generation (G4) Class 3 PCA (ECC Universal Root CA) includes a 384 bit ECC key.

All Classes of STN and Certsuperior PCAs and CAs, and RAs and end entity certificates use either SHA-1 or SHA-2 for digital signature hash algorithm and certain versions of Symantec Processing Center support the use of SHA-256 and SHA-384 hash algorithms in end-entity Subscriber Certificates.

Key sizes for Certsuperior EV certificates are identified in Appendix B2.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Refer to Section 7.1.2.1.

6.2 *Private Key Protection and Cryptographic Module Engineering Controls*

Certsuperior has implemented a combination of physical, logical, and procedural controls to ensure the security of Certsuperior and Enterprise Customer CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, Certsuperior uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 Level 3.

6.2.2 Private Key (m out of n) Multi-Person Control

Certsuperior has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. Certsuperior uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

Certsuperior creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

Certsuperior does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12. For ACS Application IDs, Certsuperior does not store copies of Subscriber private keys.

6.2.5 Private Key Archival

Upon expiration of a Certsuperior CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CPS.

Certsuperior does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Certsuperior generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, Certsuperior makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

All Certsuperior sub-domain Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 Class 1 Certificates

The Standard for Class 1 private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, Certsuperior recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Class 2 Certificates

The Standard for Class 2 Private Key protection is for Subscribers to:

- Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Class 3 Certificates other than Administrator Certificates

The Standard for Class 3 private key protection (other than Administrators) is for Subscribers to:

- Use a smart card, biometric access device or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card or biometric access device in accordance with Section 6.4.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.8.4 Administrators' Private Keys (Class 3)

The Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with Section 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

Certsuperior recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.5 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.8.6 Private Keys Held by Processing Centers (Class 1-3)

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

Certsuperior CA private keys are deactivated upon removal from the token reader. Certsuperior RA private keys (used for authentication to the RA application) are deactivated upon system log off. Certsuperior RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with this CPS. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.10 Method of Destroying Private Key

Where required, Certsuperior destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. Certsuperior utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 *Other Aspects of Key Pair Management*

6.3.1 Public Key Archival

Certsuperior CA, RA and end-user Subscriber Certificates are backed up and archived as part of Certsuperior's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum Operational Periods for Certsuperior Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 8 below. End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

In addition, Certsuperior CAs stop issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

<i>Certificate Issued By:</i>	<i>Validity Period</i>
PCA self-signed (1024 bit RSA)	Up to 30 years
PCA self-signed (2048 bit RSA)	Up to 50 years
PCA self-signed (256 bit ECC)	Up to 30 years
PCA self-signed (384 bit ECC)	Up to 30 years
PCA to Offline intermediate CA	Generally 10 years but up to 15 years after renewal
PCA to online CA	Generally 5 years but up to 10 years after renewal ¹⁴
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal ¹⁵
Online CA to End-user Individual Subscriber	Normally up to 2 years, but under the conditions described below, up to 6 years ¹⁶ under the conditions described below with no option to renew or re-key. After 6 years new enrollment is required.
Online CA to End-Entity Organizational Subscriber	Normally up to 6 years ¹⁷¹⁸ under the conditions described below with no option to renew or re-key. After 6 years new enrollment is required.

Table 8 – Certificate Operational Periods

Except as noted in this section, Certsuperior Sub-domain Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to six years, if the following requirements are met:

- Protection of the Subscriber key pairs in relation to its operational environment for Organizational Certificates, operation within the enhanced protection of a data center and for Individual Certificates, the Subscribers' key pairs reside on a hardware token, such as a smart card,
- Subscribers are required to undergo re-authentication at least every 3 years under Section 3.2.3,
- Subscribers shall prove possession of the private key corresponding to the public key within the Certificate at least every 25 months under Section 3.2.3,
- If a Subscriber is unable to complete re-authentication procedures successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall revoke the Subscriber's Certificate.

Certsuperior also operates a Secure Server CA as a legacy self-signed issuing root CA which is part of the Symantec Trust Network and has an operational period of up to 15 years. End-user Subscriber Certificates issued by this CA meet the requirements for CA to end-user Subscriber Certificates specified in Table 8 above.

¹⁴ The Symantec Onsite Administrator CA-Class 3 has a validity beyond 10 years to support legacy systems and shall be revoked when appropriate

¹⁵ If 6-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. CA re-key will be required after 5 years.

¹⁶ If 6-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. CA re-key will be required after 5 years.

¹⁸ At a minimum, the Distinguished Name of certificates issued with a validity of more than 3 years is re-verified after three years from date of certificate issuance. With the exception of the Symantec Automated Administration certificate, Organizational end-entity certificates used solely to support the operation of a portion of the STN may be issued with a validity period of 5 years and up to a maximum of 10 years after renewal.

The Symantec Class 3 International Server CA is an online CA signed by a PCA. The validity of this CA may exceed the validity periods described in Table 8 above in order to meet certain contractual obligations with browser vendors regarding the use of SGC/step up technology, and ensure continued interoperability of certificates offering this capability.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing Symantec CA private keys is generated in accordance with the requirements of CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

Symantec RAs are required to select strong passwords to protect their private keys. Symantec's password selection guidelines require that passwords:

- be generated by the user;
- have at least fifteen characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

Certsuperior strongly recommends that Enterprise Administrators, RAs, and end-user Subscribers choose passwords that meet the same requirements. Certsuperior also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

Certsuperior Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

Certsuperior RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

Certsuperior strongly recommends that Client Administrators, RAs and end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, STN Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, Certsuperior shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

Certsuperior performs all CA and RA functions using Trustworthy Systems that meet the requirements of Symantec's SAR Guide. Enterprise Customers must use Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

Certsuperior ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, Certsuperior limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

Certsuperior's production network is logically separated from other components. This separation prevents network access except through defined application processes. Certsuperior uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

Certsuperior requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. Certsuperior requires that passwords be changed on a periodic basis.

Direct access to Certsuperior databases supporting Certsuperior's CA Operations is limited to Trusted Persons in Certsuperior's Production Operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by Certsuperior in accordance with Certsuperior systems development and change management standards. Certsuperior also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with Certsuperior system development standards.

Symantec developed software, when first loaded, provides a method to verify that the software on the system originated from Symantec or Certsuperior, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

Certsuperior has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Certsuperior creates a hash of all software packages and Certsuperior software

updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, Certsuperior validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

Certsuperior performs all its CA and RA functions using networks secured in accordance with the Symantec SAR Guide to prevent unauthorized access and other malicious activity. Certsuperior protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certsuperior Certificates generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 9 below:

Field	Value or Value constraint
Serial Number	Unique value per Issuer DN
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC5280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC5280.
Subject DN	See CP § 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

Table 9 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

Certsuperior Certificates are X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

7.1.2 Certificate Extensions

Certsuperior populates X.509 Version 3 STN Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of private extensions is not warranted under this CP and the applicable CPS unless specifically included by reference.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The criticality field of the KeyUsage extension is generally set to TRUE for CA certificates and may be set to either TRUE, or FALSE for end entity Subscriber certificates.

Note: The non-Repudiation bit¹⁹ is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the non-Repudiation bit means. Until such a consensus emerges, the non-Repudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the non-Repudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Consequently, this CPS does not require that the non-Repudiation bit be set. It may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). Symantec and Certsuperior shall incur no liability in relation thereto.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier for the STN CP in accordance with CP Section 7.1.6 and with policy qualifiers set forth in CP Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates are populated in accordance with RFC5280 with the exception of those issued under Public Lite accounts which may optionally exclude the email address in *SubjAltName*. The criticality field of this extension shall be set to FALSE.

7.1.2.4 Basic Constraints

Certsuperior X.509 Version 3 CA Certificates BasicConstraints extension shall have the CA field set to TRUE. End-user Subscriber Certificates BasicConstraints extension shall have the CA field set to FALSE. The criticality field of this extension shall be set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

Certsuperior X.509 Version 3 CA Certificates shall have a "pathLenConstraint" field of the BasicConstraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to an online Enterprise Customer issuing end-user Subscriber Certificates shall have a "pathLenConstraint" field set to a value of "0" indicating that only an end-user Subscriber Certificate may follow in the certification path.

¹⁹ The non-Repudiation bit may also be referred to as ContentCommitment in Digital Certificates in accordance with the X.509 standard

7.1.2.5 Extended Key Usage

By default, ExtendedKeyUsage is set as a non-critical extension. STN CA Certificates do not include the ExtendedKeyUsage extension.

7.1.2.6 CRL Distribution Points

Most Certsuperior X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

Certsuperior generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where Certsuperior populates X.509 Version 3 STN Certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC5280. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

Certsuperior Certificates are signed using one of following algorithms.

- **sha256withRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- **ecdsa-with-Sha384** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- **sha-1WithRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- **md5WithRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

Certificate signatures produced using these algorithms shall comply with RFC 3279. Either **sha-1WithRSAEncryption** or **sha256WithRSAEncryption** will be used over **md5WithRSAEncryption**²⁰.

7.1.4 Name Forms

Certsuperior populates STN Certificates with an Issuer and Subject Distinguished Name in accordance with Section 3.1.1.

²⁰ **md5WithRSAEncryption** is used only with prior approval to preserve business continuity of legacy applications.

In addition, Certsuperior may include within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement are permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended, or if a pointer to the applicable Relying Party Agreement is included in the policy extension of the certificate.

7.1.5 Name Constraints

No stipulation

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in the STN CP (see STN CP detail at: <https://www.symantec.com/content/en/us/about/media/repository/stn-cp.pdf>). Section 1.2. For legacy Certificates issued prior to the publication of the STN CP which include the Certificate Policies extension, Certificates refer to the STN CPS (see STN CPS detail at: <https://www.symantec.com/content/en/us/about/media/repository/stn-cps.pdf>).

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Certsuperior generally populates X.509 Version 3 STN Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the Certsuperior CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

CRLs contain the basic fields and contents specified in Table 13 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279.
Issuer	Entity who has signed and issued the CRL.
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.4.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 13 – CRL Profile Basic Fields

7.2.1 Version Number(s)

Certsuperior supports both X.509 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

No stipulation

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. Certsuperior validates:

- Class 2 Enterprise certificates the Enterprise OCSP which conforms to RFC 2560, and
- Class 2 Enterprise certificates and Class 3 organization certificates using the Symantec Trusted Global Validation protocol (TGV) which conforms to RFC 5019.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC 2560 and Version 1 of the OCSP specification as defined by RFC 5019 are supported.

7.3.2 OCSP Extensions

The TGV Service uses secure timestamp and validity period to establish the current freshness of each OCSP response. Certsuperior does not use a nonce to establish the current freshness of each OCSP response and clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8. Compliance Audit and Other Assessments

An annual WebTrust for Certification Authorities (or equivalent) examination is performed for Certsuperior's data center operations and key management operations supporting Certsuperior's public and Managed PKI CA services including the STN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in Section 1.3.1. Customer-specific CAs are not specifically audited as part of the audit of Certsuperior's operations unless required by the Customer. Certsuperior shall be entitled to require that Enterprise Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

In addition to compliance audits, Certsuperior shall be entitled to perform other reviews and investigations to ensure the trustworthiness of Certsuperior's Sub-domain of the STN, which include, but are not limited to:

- Certsuperior shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event Certsuperior has reason to believe that the audited entity has failed to meet STN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the STN.
- Certsuperior shall be entitled to perform "Supplemental Risk Management Reviews" on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

Certsuperior shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with Certsuperior and the personnel performing the audit, review, or investigation.

8.1 *Frequency and Circumstances of Assessment*

Compliance Audits are conducted at least annually at the sole expense of the audited entity.

8.2 *Identity/Qualifications of Assessor*

Certsuperior's CA compliance audits are performed by a public accounting firm that:

- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and
- Is accredited by the American Institute of Certified Public Accountants (AICPA), which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

8.3 *Assessor's Relationship to Assessed Entity*

Compliance audits of Certsuperior's operations are performed by a public accounting firm that is independent of Certsuperior.

8.4 *Topics Covered by Assessment*

The scope of Certsuperior's annual WebTrust for Certification Authorities (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 *Actions Taken as a Result of Deficiency*

With respect to compliance audits of Certsuperior's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by Certsuperior management with input from the auditor. Certsuperior management is responsible for developing and implementing a corrective action plan. If Certsuperior determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the STN, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, Certsuperior Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 *Communications of Results*

A copy of Certsuperior's WebTrust for CA (or equivalent) audit report can be found at <http://www.Certsuperior.com/repository>.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Certsuperior, is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

Certsuperior does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

Certsuperior does not charge a fee as a condition of making the CRLs required by this CP available in a repository or otherwise available to Relying Parties. Certsuperior is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. Certsuperior does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without Certsuperior's prior express written consent.

9.1.4 Fees for Other Services

Certsuperior does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Within Certsuperior's Sub-domain, the following refund policy (reproduced at <http://www.Certsuperior.com/repository/refund/>) is in effect:

Certsuperior adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that Certsuperior revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that Certsuperior revoke the certificate and provide a refund if Certsuperior has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate. After Certsuperior revokes the subscriber's certificate, Certsuperior will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via check, for the full amount of the applicable fees paid for the certificate. To request a refund, please call customer service at +52(55)59855000- This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. Certsuperior maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. Certsuperior's financial resources are set forth in disclosures appearing at: www.certsuperior.com

9.2.3 Extended Warranty Coverage

No Stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by Symantec or a Customer,
- Audit reports created by Certsuperior or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of Certsuperior hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, Certsuperior repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

Certsuperior secures private information from compromise and disclosure to third parties.

9.4 *Privacy of Personal Information*

9.4.1 Privacy Plan

Certsuperior has implemented a privacy policy, which is located at: www.Certsuperior.com/privacy/index.html, in compliance with CP § 9.4.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information

STN participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Certsuperior shall be entitled to disclose Confidential/Private Information if, in good faith, Certsuperior believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 *Intellectual Property rights*

The allocation of Intellectual Property Rights among Certsuperior Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such Certsuperior Sub-domain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. Certsuperior and Customers grant permission to reproduce and distribute

Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. Certsuperior and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

STN Participants acknowledge that Certsuperior retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, Symantec's Root public keys and the Root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of Symantec. Symantec licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from Symantec.

9.6 *Representations and Warranties*

9.6.1 CA Representations and Warranties

Certsuperior warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,

- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 *Disclaimers of Warranties*

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim Certsuperior's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 *Limitations of Liability*

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit Certsuperior's liability. Limitations of liability shall include an exclusion of indirect,

special, incidental, and consequential damages. They shall also include the following liability caps limiting Certsuperior's damages concerning a specific Certificate:

Class	Liability Caps
Class 1	One Hundred U.S. Dollars (\$ 100.00 US) or equivalent in local currency
Class 2	Five Thousand U.S. Dollars (\$ 5,000.00 US) or equivalent in local currency
Class 3	One Hundred Thousand U.S. Dollars (\$ 100,000.00 US) or equivalent in local currency

Table 14 – Liability Caps

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify Certsuperior for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify Certsuperior for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10 *Term and Termination*

9.10.1 Term

The CPS becomes effective upon publication in the Certsuperior repository. Amendments to this CPS become effective upon publication in the Certsuperior repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, Certsuperior sub-domain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 *Individual Notices and Communications with Participants*

Unless otherwise specified by agreement between the parties, Certsuperior sub-domain participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 *Amendments*

9.12.1 Procedure for Amendment

Amendments to this CPS may be made by the Certsuperior Policy Management Authority (PMA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the Certsuperior Repository located at:

<https://www.Certsuperior.com/repository/updates>. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change in the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2 Notification Mechanism and Period

Certsuperior and the PMA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion.

Proposed amendments to the CPS shall appear in the Practices Updates and Notices section of the Certsuperior Repository, which is located at:

<https://www.Certsuperior.com/repository/updates>.

Notwithstanding anything in the CPS to the contrary, if the PMA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the STN or any portion of it, Certsuperior and the PMA shall be entitled to make such amendments by publication in the Certsuperior Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, Certsuperior shall provide notice to of such amendments to Certsuperior sub-domain participants.

9.12.2.1 Comment Period

Except as otherwise stated, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the Certsuperior Repository. Any Certsuperior sub-domain participant shall be entitled to file comments with the PMA up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed amendments. The PMA is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the Certsuperior Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be Changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 *Dispute Resolution Provisions*

9.13.1 Disputes among Symantec, Affiliates, and Customers

Disputes among Certsuperior sub-domain participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes involving Certsuperior require an initial negotiation period of sixty (60) days followed by litigation in Mexico, in the case of claimants who are Mexican residents or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration.

9.14 *Governing Law*

Subject to any limits appearing in applicable law, the laws of Mexico shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Mexico. This choice of law is made to ensure uniform procedures and interpretation for all Certsuperior sub-domain participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15 *Compliance with Applicable Law*

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 *Miscellaneous Provisions*

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting Symantec.

9.17 *Other Provisions*

Not applicable

Appendix A. Table of Acronyms and definitions

Table of Acronyms

Term	Definition
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAR	Security and Audit Requirements
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
STN	Symantec Trust Network.

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with Symantec to be a STN distribution and services channel within a specific territory.
Affiliate Practices Legal Requirements Guidebook	A Symantec document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a Symantec registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by Symantec that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.

Term	Definition
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	This document, which is entitled "Symantec Trust Network Certificate Policies" and is the principal statement of policy governing the STN.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the STN.
Certification Practice Statement (CPS)	A statement of the practices that Symantec or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with STN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Exigent Audit/Investigation	An audit or investigation by Symantec where Symantec has reason to believe that an entity's failure to meet STN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the STN posed by the entity has occurred.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A Symantec service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
Managed PKI	Symantec's fully integrated managed PKI service that allows enterprise Customers of Symantec and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.

Term	Definition
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CPS § 9.2.3.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	STN PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within Symantec responsible for promulgating this policy throughout the STN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (Symantec or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the STN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The STN PKI consists of systems that collaborate to provide and implement the STN.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by Symantec or an Affiliate, acting as CA, to individuals or organizations applying one by one to Symantec or an Affiliate on its web site.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server CA	The Certification Authority that issues Secure Server IDs.
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.

Term	Definition
<i>Secure Sockets Layer (SSL)</i>	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
<i>Security and Audit Requirements (SAR) Guide</i>	A Symantec document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
<i>Security and Practices Review</i>	A review of an Affiliate performed by Symantec before an Affiliate is permitted to become operational.
<i>Service Center</i>	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
<i>Sub-domain</i>	The portion of the STN under control of an entity and all entities subordinate to it within the STN hierarchy.
<i>Subject</i>	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
<i>Subscriber</i>	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
<i>Subscriber Agreement</i>	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
<i>Superior Entity</i>	An entity above a certain entity within a STN hierarchy (the Class 1, 2, or 3 hierarchy).
<i>Supplemental Risk Management Review</i>	A review of an entity by Symantec following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
<i>Reseller</i>	An entity marketing services on behalf of Symantec or an Affiliate to specific markets.
<i>Symantec</i>	Means, with respect to each pertinent portion of this CPS, Symantec Corp. and/or any wholly owned Symantec subsidiary responsible for the specific operations at issue.
<i>Symantec Digital Notarization Service</i>	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
<i>Trusted Person</i>	An employee, contractor, or consultant of an entity within the STN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
<i>Trusted Position</i>	The positions within a STN entity that must be held by a Trusted Person.
<i>Trustworthy System</i>	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
<i>Symantec Repository</i>	Symantec's database of Certificates and other relevant Symantec Trust Network information accessible on-line.
<i>Symantec Trust Network (STN)</i>	The Certificate-based Public Key Infrastructure governed by the Symantec Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by Symantec and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
<i>STN Participant</i>	An individual or organization that is one or more of the following within the STN: Symantec, an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
<i>STN Standards</i>	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the STN.